Investigating Correlation-Based Fingerprint Authentication Schemes for Mobile Devices Using the J2ME technology

Yi Wang, Jiankun Hu and Kai Xi
Royal Melbourne Institute of Technology
School of Computer Science and Technology
Melbourne, Australia 3001
Email: {alice, jiankun}@cs.rmit.edu.au, S3102841@student.rmit.edu.au

Vijayakumar Bhagavatula
Carnegie Mellon University
Department of Electrical and Computer Engineering
Pittsburgh, PA 15213
Email: kumar@ece.cmu.edu

Abstract

This paper investigates correlation-based fingerprint authentication schemes that can be used for mobile devices. The investigated algorithms were implemented with a J2ME environment on the application layer. In order to reduce the resources demanded for the mobile device environment, we also propose a new hierarchical correlation-based scheme based on the idea that the overall authentication can be decomposed into partial autocorrelations. The algorithms have been tested on a J2ME CDC 1.0 emulator of a smart mobile phone.

1. Introduction

Today, a mobile phone can be integrated with a camera, a GPRS, a radio, a MP3 player, a web browser and even a TV. It is foreseeable that future mobile devices will just be more powerful and function like hand held computers.

With this trend of convergence, potential security problems have become more threatening and harmful. This urges stronger protections against data leaking and illegitimate use of the device. Biometric authentication can ensure genuine user presence, thus enhancing the privacy protection.

Only recently, a few products of biometric-enabled mobile devices have been announced available to consumers. However, different manufacturers tend to have their own standards and proprietary technology. In most current commercial solutions, the biometric function is embedded in the system hardware and is expensive.

We consider to deploy biometric authentication in the application layer so that better extendability and portability can be achieved for general mobile devices.

Figure 1. J2ME Emulator GUI.

Our application is developed using Java 2 Micro Edition (J2ME) [2]. J2ME is a green version of Java. It inherits Java's main benefit of being platform independent as well as object oriented. Moreover, J2ME was especially designed to fit resource-constrained embedded systems. Its applications can be emulated on a PC during the development stage and then easily uploaded to PDAs or mobile phones, without the need of expensive system-specific kits and hardware.

1-4244-1300-1/07/$25.00 2007 IEEE

Figure 1 shows a J2ME emulator GUI of a commercial mobile terminal.

J2ME applications should be designed to consume as little resource as possible. To meet this special requirement, we develop a new hierarchical correlation algorithm for fingerprint authentication on mobile devices. The proposed scheme consumes less memory resource than a full-sized image correlation. To investigate the authentication performance, a worst case scenario for the correlation-based algorithms was considered where fingerprints with plastic distortions are used for testing in our experiments.

The rest of the paper is organized as follows. Section 2 presents the proposed hierarchical correlation-based fingerprint authentication. Section 3 discusses related issues of the J2ME implementation. Section 4 provides experimental results, and finally we conclude in section 5.

2. Hierarchical Fingerprint Authentication

Most existing algorithms for fingerprint matching are based on ridge endings and bifurcations (minutiae) [5]. In those schemes, authentication is approved only if the number of matched minutiae exceeds a predefined threshold. For mobile devices, the fingerprint sensor is usually quite small. Hence, partial and non-overlapping fingerprints are often obtained. This tends to reduce the performance of a minutiae-based fingerprint matching approach. Moreover, minutiae-based algorithms often require a few intermediate image processing steps such as orientation extraction [7, 8] and ridge thinning [1], which will increase the complexity of the J2ME application on mobile devices.

The correlation-based fingerprint matching uses overall information provided in a fingerprint image. A synthetic filter is often built as a template using a number of training examples [3]. When a test fingerprint perfectly matches with the filter (template), a well-defined peak will appear in the resulting correlation plane. Otherwise, a flat correlation output is expected to be observed.

2.1. Minimum average correlation energy (MACE) filter

The MACE filter [4] was designed to suppress the sidelobes of correlation plane such that a sharp correlation peak can be produced. Assuming N training images of a subject, each image has a total of d pixels. For the i'th training image, the columns of its 2D Fourier transform is concatenated to form a column vector $\mathbf{x_i}$ containing d elements. A matrix X from N training images is then defined as

$$\mathbf{X} = [\mathbf{x_1}, \mathbf{x_2} \cdots \mathbf{x_N}]^T.$$

The 2D MACE filter obtained in the frequency domain is also ordered in a column vector $\mathbf{h}$. The i'th correlation output at the origin is constrained to a prespecified value u_i, which can be represented as

$$c(0) = \mathbf{x}_i^+ \mathbf{h} = \mathbf{h}\mathbf{x}_i^+ = u_i, \tag{1}$$

where the superscript '$+$' denotes a conjugate transpose. Note that $c(0)$ is also referred to the correlation peak value.

On the other hand, based on Parseval's theorem, the average of the correlation plane energies, $\mathbf{E}_{ave}$, can be obtained directly from the frequency domain by

$$\begin{aligned} \mathbf{E}_i &= \sum_{p=1}^{d} |c_i(p)|^2 = \sum_{k=1}^{d} |\mathbf{h}(k)|^2 |\mathbf{x}_i(k)|^2 = \mathbf{h}^+ \mathbf{x}_i \mathbf{x}_i^* \mathbf{h} \\ \mathbf{E}_{ave} &= \frac{1}{N} \sum_{i=1}^{N} \mathbf{E}_i = \mathbf{h}^+ \Big[\frac{1}{N} \sum_{i=1}^{N} \mathbf{x}_i \mathbf{x}_i^* \Big] \mathbf{h} = \mathbf{h}^+ \mathbf{D} \mathbf{h} \end{aligned} \tag{2}$$

where the superscript '$*$' denotes complex conjugation and D is a diagonal matrix of size $d \times d$ whose diagonal elements are the power spectrum of $\mathbf{x}_i$.

Minimizing the average correlation energy $\mathbf{E}_{ave}$ subjecting to the constraints placed in (1) leads to the MACE filter solution

$$\mathbf{h} = \mathbf{D}^{-1}\mathbf{X}(\mathbf{X}\mathbf{D}^{-1}\mathbf{X})^{-1}\mathbf{u}, \tag{3}$$

where $\mathbf{u} = [u_1, u_2, ..., u_N]^T$.

2.2. Hierarchical correlation-based authentication

Conventional correlation-based authentications use full-sized fingerprint images. It has been reported that down-sampling 500dpi images to 256×256 pixels results in better performance compared to other resolutions [6]. However for mobile devices, this still consumes too much memory and computing power. Therefore, we consider to use partial images at each time of correlation computation.

Let us first consider a simple 1D case. In the space domain, correlation of $r[k]$ with a target $t[k]$ leads to the following correlation output

$$c(l) = \sum_{k=1}^{N} r[k]t[k-l]. \tag{4}$$

As the correlation output is a sum of inner products in the range of $[1, N]$, we see that given $1 < a < N$,

$$c(l) = \sum_{k=1}^{a} r[k]t[k-l] + \sum_{k=a+1}^{N} r[k]t[k-l]. \tag{5}$$

Let us now determine the mean of the correlation output at the origin, especially for the case $r[k] = t[k]$ when both

(4) and (5) reduce to autocorrelations. From (4), we have

$$E\{c(0)\} = E\Big\{\sum_{k=1}^{N} r[k]t[k]\Big\} = \sum_{k=1}^{N} E\{t[k]^2\} = NE\{t[k]^2\} = NR[0], \tag{6}$$

where $R[0]$ is the autocorrelation function of $t[k]$ at the origin. From (5), we have

$$\begin{aligned} E\{c(0)\} &= E\Big\{\sum_{k=1}^{a} r[k]t[k] + \sum_{k=a+1}^{N} r[k]t[k]\Big\} \\ &= E\Big\{\sum_{k=1}^{a} r[k]t[k]\Big\} + E\Big\{\sum_{k=a+1}^{N} r[k]t[k]\Big\} \\ &= \sum_{k=1}^{a} E\{t[k]^2\} + \sum_{k=a+1}^{N} E\{t[k]^2\} \\ &= aR[0] + (N-a)R[0] = NR[0] \end{aligned} \tag{7}$$

The above evaluation can be easily extended for 2D cases. It clearly shows that for autocorrelation, the output peak at the origin is equal to the sum of peak values obtained from the corresponding fractions of the original segment. If the fractions are from other sources, the difference between the peak sum and the original peak value from the target source will not be zero. Based on this idea, we propose a correlation-based hierarchical fingerprint authentication scheme as shown in Figure 2.

The key modules in Figure 2 are described as follows. In the enrollment stage, a template is constructed (possibly offline) from a set of training images based on the MACE filter design as described previously in section 2.1. The template is represented in the space domain and will be stored in the mobile device.

In the authentication stage, three donut rings will be first extracted from the test fingerprint's core center by defining three concentric circles. For example as shown in Figure 3, the inner donut ring $\mathbf{R}_1$ is defined by concentric circles C_1 and C_2. The outer donut ring $\mathbf{R}_2$ is defined by C_2 and C_3. The overall donut ring $\mathbf{R}_3$ is defined by C_1 and C_3. Corresponding parts in the template will also be extracted using concentric circles with the same diameters, namely $\mathbf{T}_1$, $\mathbf{T}_2$ and $\mathbf{T}_3$.

The donut rings $\mathbf{R}_1$, $\mathbf{R}_2$ and $\mathbf{R}_3$ from the test fingerprint are then correlated with their corresponding template parts $\mathbf{T}_1$, $\mathbf{T}_2$ and $\mathbf{T}_3$ respectively, yielding three correlation peak values p_1, p_2 and p_3. Let

$$d' = p_3 - (p_1 + p_2). \tag{8}$$

The difference can also be normalized to

$$d = d'/p_3 = 1 - (p_1 + p_2)/p_3. \tag{9}$$

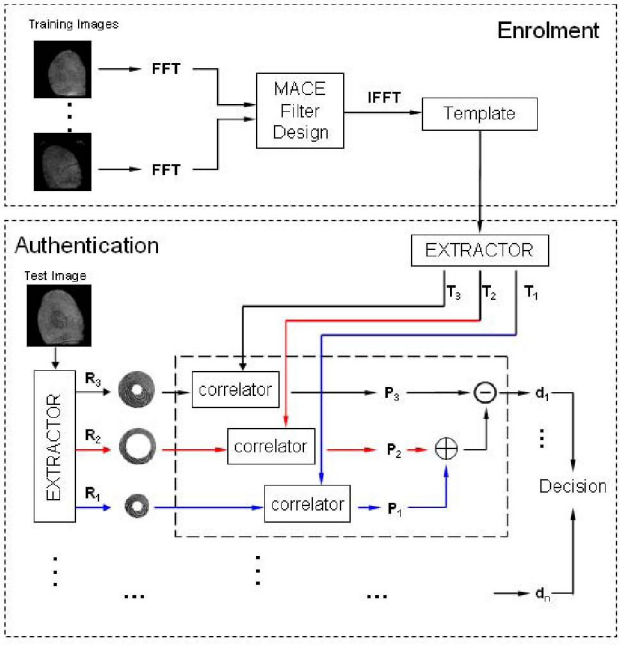

Figure 2. Schematic of the proposed hierarchical fingerprint authentication.

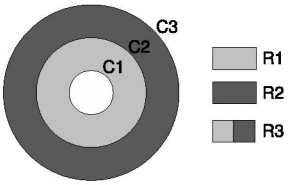

Figure 3. Using concentric circles C1, C2, C3 to extract parts R1, R2, R3 in a test fingerprint.

Ideally, d will be close to zero when the test fingerprint is from the same source of the template and be large otherwise. However in practice, the difference value d will not be zero due to distortions presenting in fingerprints. In fact, the difference increases when the deformation goes larger.

To address this problem, we use a set of repetitions of the hierarchical correlation by gradually increasing the dimensions of the concentric circles. Each repetition will produce a difference measure, say d_i. The authentication decision is made on the weighted average sum of d_i. For N repetitions, it is

$$D = \frac{1}{N}\sum_{i=1}^{N} w_i d_i, \tag{10}$$

where w_i is the weighing factor for d_i in order to control the impact of distorted areas to the authentication decision.

1. Read in test fingerprints I and register.
   Load template H.
2. Initialize concentric circles C1, C2, C3 for extraction.
3. For i = 1to N
   (0) Let a <- C1, b <- C2.
   (1) Extract fractional part R from I:
   R <- extract_ring(I, a, b),
   where a defines the inner circle and b defines the
   outer circle.
   (2) Extract the corresponding part T from H:
   T <- extract_ring(H, a, b).
   (3) Calculate the correlation peak p output by R and H.
   (4) Let p1 = p;
   (5) Let a <- C2, b <- C3. Repeat (1)-(3).
   Let p2 = p.
   (6) Let a <- C1, b <- C3. Repeat (1)-(3).
   Let p3 = p.
   (7) Calculate the normalized difference
   d(i) = 1 − (p1 + p2) / p3.
   (8) Update the diameters of C1, C2, C3.
   End For.
4. Calculate the weighted average sum:
   D = 1/N Σ w(i)d(i).
5. Make a decision:
   if D < D_threshold, I is genuine;
   otherwise, I is imposer.

Figure 4. The hierarchical correlation-based algorithm.

The weighing factors can be derived from some correlation metrics such as the peak to correlation energy (PCE) value. Both plastic deformation and imposter source can result in a low PCE value. But if only partial areas are distorted in a genuine fingerprint, the weighted average sum of d_i tend to be smaller than the one from a complete imposter source by incorporating the weighing.

The test fingerprint will be authenticated if D is below a predefined threshold and be rejected otherwise. Figure 4 provides a description of the proposed correlation-based hierarchical fingerprint authentication scheme.

3. J2ME Implementation Issues

The heart of Java 2 Micro Edition (J2ME) is a compact virtual machine (VM) whose basic functionalities are summarized in *configurations*. Currently, there are two configurations available, each was defined for devices with similar computing power and equipment characteristics, namely connected limited device configuration (CLDC) and connected device configuration (CDC) [2]. Our application is built upon CDC that allows more resources to be used.

On top of a configuration, profiles are designed to add device-type-specific classes. There is another important concept termed *optional package*. A n optional package is a set of APIs in support of additional, common behaviors that do not really belong in one specific configuration or profile.

The CDC platform adopted is Sony Ericsson P990 which supports CDC 1.0 with foundation profile 1.0, personal profile 1.0 and PDA optional packages. Our application is developed using NetBeans IDE 5.0 which maintains an emulator of the CDC platform.

The CDC 1.0 provides support for floating numbers but not for complex numbers. Therefore, we write a class by ourselves to handle complex numbers generated from the FFT used in correlators. In fact, the Fast Fourier Transform (FFT) algorithm was also implemented from scratch as well. The FFT algorithm provides a computational advantage by a factor of $N^2/Nlog_2N = N/log_2N$ for N-point DFT [3]. As N increases, this FFT efficiency ratio increases greatly and so does the resource usage.

The proposed hierarchical method has a computational advantage over the conventional full correlation method in terms of memory saving. In our hierarchical scheme, the FFT is performed only on one fractional part extracted from a fingerprint image or template at one time. Therefore, the N used in the hierarchical scheme for each correlation is much smaller than that required by the full correlation. Moreover, if the weighing factor w_i from PCE is removed from (10), the hierarchical method will then require only the information of peak values at the center. Thus, even FFTs can be exempt - only the dot product of the vectors will be enough [3]. This can further speed up the correlators but will also degrade the performance of the hierarchical scheme as distortions are not in any control.

The disadvantage of the proposed scheme is its requirement of registration for test fingerprints in order to extract the corresponding parts with the template. The full correlation method does not require registration. However, it is not feasible to implement full correlation on the J2ME mobile environment as the required memory will exceed the current limit, which will be shown in section 4.

4. Experimental Results

We consider the worst case for correlation-based fingerprint matching where plastic distortion presents in the test fingerprints. The data set we adopted is from the NIST Special Database 24 [9] of live-scanned fingerprint samples. In our preliminary experiments, a subset of 10 finger subjects was chosen from the distortion set each has 300 different impressions. This results in 3,000 individual fingerprints in our experiments.

Our performance evaluation is of two stages. Firstly, the

correlation algorithms were implemented and tested on a general purpose PC. The main advantage of doing this is to exclude the restrictions of memory as well as computing power placed on mobile devices. This has allowed us to detect flaws and bottlenecks of our implementations. We then implemented the same algorithms on the J2ME CDC platform and performed tests.

In NIST Special Database 24, the live-scanned fingerprints are obtained from an optical sensor of resolution 500 dpi with original size of 720×480 pixels. The selected fingerprints were first properly cropped, downsampled via averaging and zero padded to a new size of 256×256. The fingerprints are also taken negative and registered to the image center. The images are normalized so that the energy of each image is equal to 1.

Firstly, we need to choose the training set for building the filter templates. For each finger subject, 30 impressions are uniformly sampled across the 300 available fingerprints. The rest 270 impressions are then used as genuine test images. Fingerprints from all other subjects will be regarded as imposter test images. Therefore, a total $10 \times 270 = 2700$ genuine tests and $10 \times 9 \times 300 = 27,000$ imposter tests were performed.

For the hierarchical scheme, we choose the number of repetitions, N, to be 3. The initial diameters of C_1, C_2 and C_3 are set to 0, 30 and 60 pixels respectively. The incremental size of the concentric circles is 10 in each repetition.

The system's authentication performance can be assessed by several metrics. Two commonly used ones are false acceptance rate (FAR) and false rejection rate (FRR). The FAR is defined as the error rate of an imposter being falsely accepted by the system, while the FRR is the error rate of a genuine user being falsely rejected. When the two error rates are equal, the common value is referred to as the equal error rate (EER).

Figure 5 plots the FAR and FRR produced by the proposed hierarchical correlation method with different decision value of D defined in (10). As the decision value increases, the FAR increases while the FRR decreases. The EER is the value at the intersection of the two error curves.

There is a strict tradeoff between FAR and FRR in every biometric system [5]. For a verification application on a mobile device, a low FAR is more important as the primary objective is not to let in any imposter. However, a high FRR may irritate the customers by requiring a retry for several times. Therefore, we consider the EER and FRR at zero FAR as our comparison indices.

Figure 6 shows the average EER and average FRR at zero FAR for the proposed hierarchical correlation-based method and conventional correlations with different image cropping size. The cropping is conducted around the image center.

As shown in the figure, the error rates obtained by the

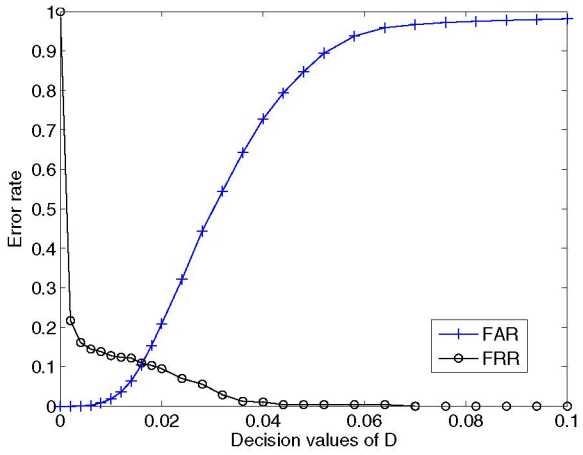

Figure 5. FAR and FRR with respect to the decision value of D.

proposed hierarchical method are lower than those obtained by conventional correlations. In particular, the FRR at zero FAR has gained large improvement from the proposed hierarchical method.

We have noticed that the error rates for all correlation-based methods are relatively high for this preliminary experiment. The small distortion data set that we chose for the test may be one of the reasons, as plastic deformation is of disadvantage for correlation-based fingerprint matching. We also need to improve our filter implementation to reduce error rates, for example, using distortion tolerant filters, in our future work. However, we consider the comparison is still fair as all the comparing correlation-based algorithms are implemented on the same platform and with the same data source as well as templates.

On the other hand, we have also examined the resource consumption of the above correlation-based algorithms. The memory available on the J2ME emulator is 100 MB. The full correlation method with original image size of 256×256 requires excessive memory than this limit of the device, thus its computation was crashed on the emulator. Table 1 summarizes the memory usage of the comparing algorithms.

64×64	128×128	256×256	Hierarchical
0.94MB	2.43MB	210MB	1.32MB

Table 1. Average memory requirement by the comparing correlation-based methods. The memory available on the J2ME CDC 1.0 emulator is about 100MB.

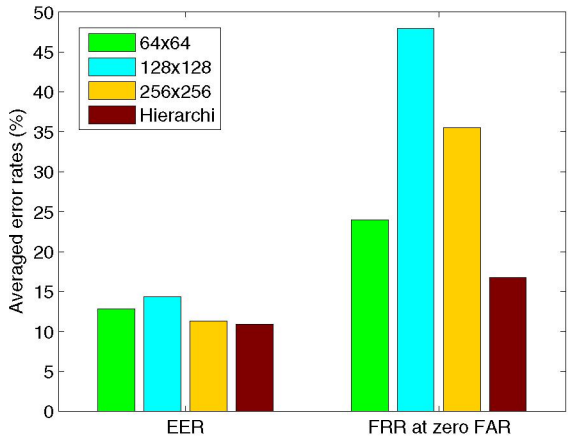

Figure 6. Average error rates from the proposed hierarchical correlation-based method and image correlations with different size.

Table 2 tabulates the authentication time that the comparing correlation-based methods required on the J2ME CDC emulator. The measure for the full correlation with image size 256×256 is not available due to memory crash.

64×64	128×128	256×256	Hierarchical
5 seconds	11 seconds	N/A	15 seconds

Table 2. Authentication time required by the correlation-based methods on the J2ME CDC emulator. The full correlation method with image size 256×256 is not available due to memory crash.

In table 1 and 2, although the partial correlation of 64×64 consumes the least memory source and is faster, we keep in mind that the error rates obtained by the proposed hierarchical method is better as shown in Figure 6.

5. Conclusions

In this paper, we have investigated the development of correlation-based algorithms for biometric authentications on mobile devices. As mobile applications are strictly subject to resource constraints, we propose a memory-saving hierarchical correlation scheme for fingerprint matching. The proposed algorithm together with the conventional full correlation method were implemented and compared on a J2ME CDC 1.0 platform.

Our preliminary experimental results show that the proposed hierarchical scheme has clear advantage in terms of memory consumption over the full correlation method. However, as there is often a tradeoff between execution speed and memory consumption [2], the proposed hierarchical method is slower than partial correlation algorithms. It is able to achieve reasonable authentication performance when plastic distortion presents in test fingerprints.

6. Acknowledgement

This work is supported by the ARC linkage project LP0455324.

References

[1] A. Jain, L. Hong, and R. Bolle. On-line fingerprint verification. *IEEE Trans. Pattern Anal. Machine Intell.*, 19(4):302–314, Apr 1997.

[2] M. Kroll and S. Haustein. *Java 2 micro edition application development*. Sams Publishing, 2002.

[3] B. V. K. V. Kumar, A. Mahalanobis, and R. Juday. *Correlation pattern recognition*. Cambridge University Press, New York, 2005.

[4] A. Mahalanobis, B. V. Kumar, and D. Casasent. Minimum average correlation energy filters. *Applied Optics*, 26(17):3633–3640, 1987.

[5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of fingerprint recognition*. Springer-Verlag, New York, 2003.

[6] K. Venkataramani and B. V. Kumar. Performance of composite correlation filters in fingerprint verification. *Optical Engineering*, 43(8):1820–1827, 2004.

[7] Y. Wang, J. Hu, and F. Han. Enhanced gradient based algorithm for the estimation of fingerprint orientation fields. *Applied Mathematics And Computation*, online Aug 2006.

[8] Y. Wang, J. Hu, and D. Phillips. A fingerprint orientation model based on 2d fourier expansion (fomfe) and its application to singular-point detection and fingerprint indexing. *IEEE Trans. Pattern Anal. Machine Intell.*, to appear in May 2007.

[9] C. Watson. Nist special database 24, live-scan digital video fingerprint database. Technical report, U.S. National Institute of Standards and Technology, 1998.